

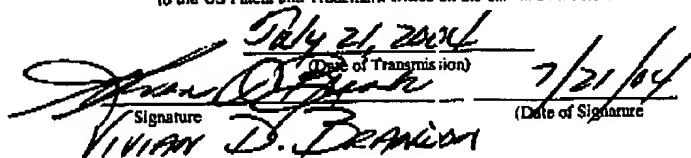
Serial No. 09/760,999

OFFICIALRECEIVED
CENTRAL FAX CENTER

JUL 21 2004

RD-28,556

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being transmitted by facsimile
to the US Patent and Trademark Office on the date shown below:

July 21 2004
John D. Bernick (Date of Transmission)
Signature
Vivian D. Bernick (Date of Signature)

PAGES FAXED=5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: Barnett et al.

Serial No.: 09/760,999

Group Art Unit: 2157

Filed: January 16, 2001

Examiner: El Chanti

Title: Delegated Administration Of Information
In A Database Directory Using Attribute Permissions Response to Paper No.: 6REQUEST FOR RECONSIDERATION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 2213-1450

Sir:

Applicant carefully considered the Office Action mailed on April 22, 2004. Claims 1-30 are pending in the present patent application. Of the pending claims, the Examiner rejected claims 1-30. Applicant requests further examination and reconsideration of the present patent application.

The Examiner rejected claims 1-4, 7, 10-21, 25 and 28 under 35 USC §102(e) as being anticipated by Jerger et al. (US Patent No. 6,321,334). Applicant respectfully traverses the §102(e) rejection of the present patent application and submits that Jerger et al. (hereinafter Jerger) does not anticipate the claimed invention.

In one form or another, all of the independent claims (i.e., 1, 4, 7, 10, 16, 21, 25 and 28) of the present invention recite a user community where user information is managed.

Serial No. 09/760,999

RD-28,556

defining a set of user attributes for each user in the user community and identifying a permission level for managing the user attributes. Examples of a "user attribute" as provided in page 6, lines 19-21, of the present patent application, include employer, role or job description, resources that permission has been granted to access, address and equipment used.

Jerger does not disclose teachings that recite a user community where user information is managed, defining a set of user attributes for each user in the user community and identifying a permission level for managing the user attributes. The Examiner referenced col. 3, lines 9-15 as being relevant to defining a set of user attributes for each user in a user community and providing user information associated with the user community to the administrator. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of defining a set of user attributes for each user in a user community and providing user information associated with the user community to the administrator as it is discussed in the present patent application. Instead, col. 3, lines 9-15 discusses configuring a system security policy to establish multiple security zones wherein each security zone corresponds to a set of locations on a computer network. Further, this section discusses that each zone has a corresponding security configuration that specifies the actions to be taken when a protected operation is requested by active content downloaded from that security zone. The teaching in this section is not analogous to the claimed limitation because there is no mention of a user community where user information is managed and defining a set of user attributes for each user in the user community. Jerger does not teach this limitation because this patent is not concerned with managing user information for a user in a user community. Instead, Jerger is only interested in managing active content downloaded from a computer network and using a system security policy that protects a user's computer from potentially harmful active content received from a server computer.

The Examiner suggested that col. 3, lines 16-26 in Jerger is relevant to identifying a permission level for managing each of the user attributes. Applicant carefully reviewed this section and submits that it does not anticipate the claimed limitation of identifying a permission level for managing user attributes. Instead, this section pertains to a mechanism to determine the security zone corresponding to a network location. Further, this section

Serial No. 09/760,999

RD-28,556

describes a mechanism to determine an action to perform based on the Web site's security zone, the requested operation and the security setting corresponding to the requested operation and the Web site's zone. The teaching in this section is not analogous to the claimed limitation because there is no mention of identifying a permission level for managing user attributes. Jerger does not teach this limitation because this patent is not concerned with managing user information for a user in a user community and identifying a permission level for managing the user attributes.

The Examiner suggested that col. 3, lines 55-65 in Jerger is relevant to managing user attributes according to each of the permission levels. Applicant carefully reviewed this section and submits that it does not anticipate the claimed limitation of managing user attributes according to permission levels. Instead, this section pertains to a system security policy having a number of security zones, wherein each zone has a zone security configuration that is enforced by a security manager application on the user's computer system. The teaching in this section is not analogous to the claimed limitation because there is no mention of managing "user attributes" according to permission levels. Jerger does not teach this limitation because this patent is not concerned with managing user information/attributes for a user in a user community, identifying a permission level for managing each of the user attributes and managing user attributes according to each of the permission levels.

Therefore, Applicant submits that the claimed invention as recited in independent claims 1, 4, 7, 10, 16, 21, 25 and 28 and as interpreted in light of the description provided in the specification is patentably distinguishable over Jerger. In particular, Jerger does not anticipate the claim limitations associated with defining a set of user attributes for each user in a user community and identifying a permission level for managing user attributes when read in light of the specification. Accordingly, Applicant submits that Jerger does not anticipate claims 1, 4, 7, 10, 16, 21, 25 and 28.

Claims 2, 3; 5, 6; 8, 9; 11-15; 17-20; 22-24; 26-27; and 29-30 depend directly or indirectly from now presumably allowable claims 1, 4, 7, 10, 16, 21, 25 and 28, respectively, and thus are allowable by dependency. Below is a summary of some of the distinctions between these depending claims and Jerger.

Serial No. 09/760,999

RD-28,556

Claims 2, 5, 8, 12, 19, 23, 26 and 29 recite that each permission level defines administrative operations that an administrator can and cannot perform on a user attribute. Applicant carefully reviewed the material in col. 3, lines 27-41 referenced by the Examiner and submits that this section does not anticipate the claimed limitation of permission levels that define administrative operations that an administrator can and cannot perform on a user attribute. Instead, the discussion in col. 3, lines 27-41 relates to the performing of a protected operation by a document on a client computer. The section further relates to determining a security setting corresponding to the security zone from which the document was retrieved, in order to perform the protected operation. The teaching in this section is not analogous to the claimed limitation because there is no mention of permission levels that define administrative operations that an administrator can and cannot perform on a user attribute. Jerger does not teach this limitation because this patent is not concerned with permission levels that define administrative operations that an administrator can and cannot perform on a user attribute. Accordingly, Applicant submits that claims 2, 5, 8, 12, 19, 23, 26 and 29 are patentably distinguishable over Jerger.

Claims 3, 6, 9, 13, 20, 24, 27 and 30 recite defining restricted values that an administrator can assign for the user attributes. Applicant carefully reviewed the material in col. 3, lines 55-65 and col. 3, lines 42-57 referenced by the Examiner and submits that these sections do not anticipate the claimed limitation of defining restricted values that an administrator can assign for the user attributes. Instead, the discussion in col. 3 lines 55-65 relates to a system security policy having a number of security zones, wherein each zone has a zone security configuration that is enforced by a security manager application on the user's computer system. Further, the discussion in col. 3, lines 42-57 referenced by the Examiner relate to modes of configurations of the client computer, the browser and the server computer. The teaching in these sections are not analogous to the claimed invention because there is no mention of restricted values that an administrator can assign to the user attributes. Jerger does not teach this limitation because this patent is not concerned with defining restricted values that an administrator can assign for the user attributes. Accordingly, Applicant submits that claims 3, 6, 9, 13, 20, 24, 27 and 30 are patentably distinguishable over Jerger.

Serial No. 09/760,999

RD-28,556

In view of the above-noted distinctions, Applicant submits that claims 1-4, 7, 10-21, 25 and 28 are patentably distinguishable over Jerger. Accordingly, Applicant requests that the Examiner reconsider and remove the §102(e) rejection of claims 1-4, 7, 10-21, 25 and 28 under Jerger.

In view of the foregoing remarks, Applicant requests that the Examiner reconsider this application and allow claims 1-30.

If the Examiner has any questions regarding the present patent application, the Examiner can call Applicant's attorney, David Goldman, at telephone number (518)-387-5927 or (518)-387-5903.

Respectfully submitted,

(David Goldman)

David C. Goldman
Attorney for Applicant
Registration No. 34,336

Schenectady, New York

Dated: July 21, 2004